Title (en)

Random number generation method in a portable data carrier

Title (de)

Verfahren zum Erzeugen von Zufallszahlen in einem tragbaren Datenträger

Title (fr)

Procédé de génération de nombres aléatoires dans un support de données portable

Publication

EP 1569089 A2 20050831 (DE)

Application

EP 05003237 A 20050216

Priority

DE 102004008178 A 20040219

Abstract (en)

Method for generating random numbers in a portable data carrier (1) in which the random numbers are generated from a pseudo- random part and a random part. The pseudo-random part is produced using a pseudo-random number generator (9) implemented by an algorithm running in the data carrier. The random part is generated using a random number generator (5) that forms part of the hardware of the data carrier. An independent claim is made for a portable data carrier with pseudo-random and random number generators.

Abstract (de)

Die Erfindung betrifft ein Verfahren zum Erzeugen von Zufallszahlen (y1,..., ym) in einem tragbaren Datenträger (1). Das erfindungsgemäße Verfahren zeichnet sich dadurch aus, dass die Zufallszahlen (y1,..., ym) jeweils aus einem pseudozufälligen Anteil (x1,..., xm) und einem zufälligen Anteil (r1,..., rm) erzeugt werden. Der pseudozufällige Anteil wird mittels eines Pseudozufallszahlengenerators (9) ermittelt, der als ein im tragbaren Datenträger (1) implementierte Algorithmus ausgebildet ist. Der zufällige (r1,..., rm) Anteil wird mittels eines Zufallszahlengenerators (5) ermittelt, der Bestandteil der Hardware des tragbaren Datenträgers (1) ist. <IMAGE>

IPC 1-7

G06F 7/58

IPC 8 full level

G06F 7/58 (2006.01); **G07C 15/00** (2006.01); **G07F 7/10** (2006.01)

CPC (source: EP)

G06F 7/58 (2013.01); **G06F 7/588** (2013.01); **G06Q 20/341** (2013.01); **G06Q 20/40975** (2013.01); **G07C 15/006** (2013.01); **G07F 7/1008** (2013.01); **G07F 7/1016** (2013.01); **H04L 9/0625** (2013.01); **H04L 9/0861** (2013.01)

Citation (applicant)

WO 0075761 A1 20001214 - GEN INSTRUMENT CORP [US], et al

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU MC NL PL PT RO SE SI SK TR

DOCDB simple family (publication)

EP 1569089 A2 20050831; **EP 1569089 A3 20070328**; DE 102004008178 A1 20050901

DOCDB simple family (application)

EP 05003237 A 20050216; DE 102004008178 A 20040219